

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:

1234WJWJ@GMAIL.COM

MAINTAINED BY GOOGLE, INC.

1600 AMPHITHEATER PARKWAY

MOUNTAIN VIEW, CA 94043

)

)

) Magistrate No. 19-61ms

)

) [UNDER SEAL]

)

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

I, Jason Adams, a Special Agent (SA) with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to the Pittsburgh, Pennsylvania Office. I have been so employed since July 2009. As part of my duties as an HSI Special Agent, I investigate criminal violations relating to high technology crime, cyber-crime, child exploitation and child pornography including violations pertaining to the illegal distribution, receipt, possession, and production of materials depicting the sexual exploitation of children. I have received training in the area of child exploitation offenses and computer forensic examinations. I have conducted and assisted in numerous child exploitation investigations and I have executed numerous Search Warrants related to child exploitation investigations. In this regard, I have reviewed extensive samples of child pornography, including videos, photographs, and digital reproductions of photographs or other print media. I am also responsible for enforcing federal criminal statutes involving immigration and customs violations.

2. The statements in this affidavit are based in part on information provided by other HSI agents and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a Search Warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt/distribution of a visual depiction of a minor engaged in sexually explicit conduct); and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct), are presently contained in information associated with the e-mail account **1234wjwj@gmail.com**.

STATUTORY AUTHORITY

3. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting or shipping, or attempting or conspiring to transport or ship, any visual depiction using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer or mail, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or

transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

DEFINITIONS

4. The following definitions apply to this Affidavit and Attachment A:

a. “Anime,” as used herein, refers to refers to Japanese-style cartoon animation that is characterized by colorful graphics, vibrant characters, and fantastical themes, which may or may not include depictions of minors engaged in sexually explicit conduct.

b. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not

necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

e. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard

drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. “File Transfer Protocol” (“FTP”) is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP, built on client-server architecture, uses separate control and data connections between the client and the server.

h. A “hash value” is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file’s

content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

i. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

k. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

m. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

n. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

o. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

p. A “website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (“HTML”) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (“HTTP”).

q. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

PROBABLE CAUSE

Initiation of Investigation and Overview of “Website M”

5. In March 2012, HSI Phoenix initiated an investigation into a password-protected, fee-based website, identified herein as “Website M,”¹ following an interview with a Website M user (“S1”) in connection with a separate child exploitation investigation. S1 allowed HSI agents to assume S1’s online identity on Website M, and provided agents with S1’s username and password.²

6. A user can only locate and access Website M if the user knows its current web address. Once the user enters the correct web address, a box appears that requires the user to enter a “user name” and “password.” The user cannot access the site without first entering that information. Once the user enters a valid username and password, Website M’s home page appears. The opening page depicts nude anime (i.e., drawings, sketches or cartoons) lasciviously displaying their genitals. The term “Private Club” also appears on the home page

¹ Law enforcement knows the actual name of Website M. However, the investigation into users of Website M remains ongoing, and public disclosure of Website M’s actual name would potentially alert its members to the investigation, likely provoking members to notify other members of the investigation, to flee, and/or to destroy evidence. Accordingly, to preserve the confidentiality and integrity of the ongoing investigation, the actual name and other identifying details of Website M remain undisclosed in this affidavit.

² S1 provided SAs with the web address for Website M and S1’s login information to Website M but S1 has not provided sufficient information to law enforcement to understand how S1 originally obtained the web address or login information for Website M.

7. Several interviewed Website M members have told agents that they received an e-mail message inviting them to join the site and set up a username and password after they purchased child erotica from another website. Following that purchase, they received a sample image of hardcore child pornography along with the question “Are you interested in seeing more of this?” When they clicked “yes,” Website M sent them another email with instructions of how to access and join the website.

8. After gaining access to Website M by using S1’s user name and login, HSI Phoenix agents determined that it advertises files of child pornography for purchase. Once logged in as a member, the user sees the names of folders available for purchase, which contain previews or samples of images contained in the folders. As of March 2012, the website advertised that it offered 600,000 images and 400 hours of video. Such images and videos are organized into folders, the contents of which can be accessed after downloading them by purchasing a password. At all times relevant to this investigation, Website M hosted its content on a server physically located outside of the United States.

9. Throughout HSI’s investigation, Website M has typically charged between \$40 USD and \$110 USD to purchase the password for encrypted archive files containing multiple images and/or videos of child pornography and child erotica. The majority of archive files cost \$89 USD.³ Once downloaded, the user can “decrypt” the selected archive file by entering in the purchased password to reveal multiple images and/or video files. Phoenix HSI Special Agents have made undercover purchases or accessed several archive files available for purchase, which

³ A digital archive file is used to store multiple files within a single, compressed file, which can make it easier to store and transmit numerous files at the same time. File extensions associated with digital archive files include “.rar” and “.zip.”

revealed that most of the archive files contained between 500 and 2,000 image and/or video files, the majority of which are child pornography.

10. Investigating agents also found that Website M allows members to preview “samples” of the images/videos contained in an archive folder prior to purchase. Investigating agents visited Website M and previewed more than 100 sample folders. Agents found that the majority of the images and videos found in the sample or preview folders depicted apparent minors, and many depicted what appeared to be pre-pubescent minors engaged in sexual activity with adults and/or posed in a sexually explicit manner.

11. Over the course of their investigation, which has involved previewing “samples” and then downloading multiple archive files via Website M, investigating agents have found that the “sample” images and/or video screenshots corresponded to the full sets of image and video files contained in downloaded archive files.

12. After selecting an archive file for purchase, the member pays for its password via credit card. Website M then automatically sends an email to the member with the encryption password for the archive. The member must first download the archive file to a digital device and enter that password to decrypt and de-compress it.

Undercover Purchases Confirmed “Website M” Sells Child Exploitative Material

13. As noted above, HSI obtained membership information to Website M via a consensual takeover of S1’s account. Between April 2014 and May 2017, investigating agents made multiple undercover purchases of archive files from Website M.

14. For example, in April 2014, investigating agents (posing as S1) successfully downloaded archive files from Website M. Review of the de-compressed image files, based upon an analysis of hash values, determined that the purchased files included video and image

files from a series of images that the National Center for Missing and Exploited Children has identified and verified to depict a pre-pubescent minor child who appears to be less than ten years of age at the time the image was made. Purchased files included the following: “180-2.AVI 9Yo Jenny licked by dog. 16min./with sound.” The screenshot for this video depicts a nude, blindfolded, prepubescent female who appears to be less than ten years of age lying on her back while a dog licks her genitals. Over twenty additional pictures from the same series were included, such as an image of the same nude prepubescent female performing fellatio on a dog.

Financial Records Linked to Website M

15. On May 26, 2017, an HSI Phoenix agent, working in an undercover capacity, purchased an archive file from Website M titled “SIBERIAN MOUSE #36.” This file was selected because it was listed on the opening page as being newly added (as of January 2017) and agents verified the images within the sample folder contained images depicting apparent minors engaged in sexually explicit conduct. When the investigating agent purchased the “SIBERIAN MOUSE #36” file, the agent received a confirmation email from the email address “TheScript Support” through a payment processor based in the United States that stated, “Your order is currently being processed.”

16. HSI agents investigated the link between the U.S. based payment processor and Website M. Investigating agents identified the U.S. company as both a payment processor and online business management tool used by Website M.

17. On July 31, 2017, a federal magistrate in the District of Arizona signed a Search Warrant for the electronic data in the possession of the U.S. payment processor related to their business transactions with and on behalf of Website M.

18. On August 11, 2017, the U.S. payment processor provided several spreadsheets in compliance with the Search Warrant. One of the spreadsheets listed all the transactions the company processed on behalf of Website M. This list included over 1,000 purchases made to Website M.

Identifying WILLIAM JONES as a Purchaser of Child Exploitative Material from Website M

19. In September 2017, HSI analyzed the U.S. payment processor records and identified individuals who made multiple purchases from Website M.

20. The U.S. payment processor records indicate that WILLIAM JONES made approximately one (1) purchase from Website M on February 6, 2017.

21. According to the U.S. payment processor records, the email address to which it sent the auto-generated receipts and passwords for purchases made by WILLIAM JONES on Website M was 1234wjwj@gmail.com.

Evidence That WILLIAM JONES Downloaded Child Exploitive Material from Website M

22. Based upon the U.S. payment processor records, HSI generated the following list documenting a purchase WILLIAM JONES made via the U.S. payment processor from Website M along with identifying information linked to the purchase.

Date	File Purchased	First Name	Last Name	Phone
02/06/2017	PHP SCRIPT 19	William	Jones	814-720-7866

Email	Address	Currency	Total
1234wjwj@gmail.com	13397 S. Mosiertown Rd., Meadville, PA 16335	USD	89

23. Upon reviewing WILLIAM JONES' purchase history from the U.S. payment processor, it was noted that the file purchased was titled "PHP SCRIPT 19". Based on your

affiant's knowledge and experience regarding other investigations related to Website M, there were multiple other file's available for purchase at Website M which displayed a similar file naming convention beginning with the letters "PHP" followed by two- and three-digit numbers. Your affiant has reviewed several of these files and found that they are archive files containing images depicting minors engaging in sexually explicit conduct.

24. Based on undercover purchases from Website M, investigating agents determined that the only way someone can view the full content of the archive file selected appears to be to: 1) download the archive file from the website and 2) enter the password provided by the website, via email, after payment is verified. There does not appear to be any way to view the full content of folders within the site itself, even with a purchased password.

25. Based on undercover purchases from Website M, the investigation, and my training and experience, it appears that Website M generates a billing name for each archived file available for purchase that corresponds with the name of a commonly purchased "script," in order to disguise the actual contents of the file purchased from the payment processor or anyone else who has access to the billing statement. Note that, in the chart above, the purchase contains a title that includes the term "script." A "script" is computer code or software that makes a computer run smoother and faster. Some examples are "Perl," "JavaScript" and "PHP." Website M named each of the archive files it sells so that it would appear as if its Members purchased "scripts" instead of child pornography. The investigation further revealed that Website M registered its business with the U.S. payment processor under the name "The Scripts" in order to appear as a legitimate company.

Identification of the WILLIAM JONES

26. I reviewed the financial purchase records provided by the U.S. payment processor and noted the purchase by WILLIAM JONES listed his billing address as 13397 S. Mosiერთown Rd., Meadville, PA 16335.

27. A check with the Pennsylvania Department of Transportation on or about July 27, 2018 revealed WILLIAM JONES, with date of birth November 18, 1968, was issued Pennsylvania driver's license number 29108758 on October 28, 2017 and this license displays the address "13397 S MOSIERTOWN RD APT 2 MEADVILLE, PA 16335." A photograph of the adult male depicted in this record was obtained.

28. A check of the criminal history for WILLIAM JONES revealed he had been issued Federal Bureau of Investigation number 426814AC5 in relation to a 2003 felony conviction for child molestation and the sentence was eight (8) years. As a result, WILLIAM JONES is a registered sex offender in the state of Pennsylvania.

29. A check of the Pennsylvania sex offender registry website on July 27, 2018, revealed a Pennsylvania State Police Megan's Law Public Report that lists the primary address of WILLIAM JONES as "13397 S MOSIERTOWN RD APT 2 MEADVILLE PA 16335." The photographs in this report depict an adult male with similar facial appearance as the adult male depicted in Pennsylvania driver's license number 29108758, referred to in paragraph 27.

30. A check of public information and law enforcement databases revealed that WILLIAM JONES resided at 13397 S. Mosiერთown Rd., Meadville, PA 16335 with Ching Hsieh from approximately January of 2009 until January of 2019.

31. A check of public, law enforcement and U.S. Department of Homeland Security databases revealed that Ching Hsieh is an adult female citizen of Taiwan with date of birth

October 8, 1961. Records also indicate Ching Hsieh is also known as Ching Hsieh-Jones and Meg Jones. A photograph of the adult female depicted in these records was obtained.

32. A check of publicly-available property record information from Crawford County, PA, which encompasses Meadville, revealed that the residence located at 13397 S. Mosiertown Rd., Meadville, PA 16335 was owned by WILLIAM JONES and Ching Hsieh from approximately January of 2009 until January of 2019.

33. A check of law enforcement databases indicated WILLIAM JONES and Ching Hsieh had moved from Crawford County, PA to Somerset County, PA. A check of publicly-available property record information from Somerset County on September 18, 2019, revealed that in February of 2019, WILLIAM JONES and Ching Hsieh had purchased the residence located at 1233 Old Lincoln Highway, Stoystown, PA 15563.

34. On September 18, 2019, your affiant, HSI Special Agent Fina Abramovitz (SA Abramovitz), and additional HSI Agents, proceeded to 1233 Old Lincoln Highway, Stoystown, PA 15563. Upon knocking on the front door of the residence, Ching Hsieh answered, and your affiant and SA Abramovitz identified themselves as law enforcement officers by presenting badges and credentials. Your affiant positively identified Ching Hsieh by facial match to U.S. Department of Homeland Security photographs. Agents then asked to enter the residence to speak with Ching Hsieh and she agreed. Prior to the interview, your affiant confirmed Ching Hsieh spoke and understood the English language. Your affiant also verbally advised Ching Hsieh of her Miranda rights and that she was not under arrest and she affirmed her understanding. Your affiant then informed Ching Hsieh that Agents were present to discuss an issue related to WILLIAM JONES, the internet, financial transactions, and child exploitation. Your affiant confirmed that Ching Hsieh understood the term "child exploitation". Ching Hsieh

stated that she and WILLIAM JONES had become married while they lived in Meadville, PA and that approximately a year ago they moved to Somerset County, PA because WILLIAM JONES had found a new job in Somerset, PA. Ching Hsieh informed Agents that she was fully aware of the sex offender status of WILLIAM JONES and did not have access to his mobile telephone or his user account on their shared computer. Ching Hsieh then asked if she should call her husband, WILLIAM JONES, to come home and Agents agreed.

35. Following Ching Hsieh's telephone call to WILLIAM JONES, your affiant asked Ching Hsieh if her husband was known to carry a firearm. Ching Hsieh stated he did not but that he was given a gun and ammunition by a former tenant that owed them \$4-5,000 in past-due rent. Your affiant asked where the gun was located and Ching Hsieh stated it was in the residence, downstairs. Your affiant asked Ching Hsieh to lead Agents to the gun and ammunition and she agreed to do so. Ching Hsieh then led your affiant and SA Abramovitz to a room in the basement and identified the gun leaning against a wall and ammunition on a shelf. Agents observed the gun to be a shotgun and the ammunition to be approximately ten (10) unspent 12-gauge shotgun shells contained in a clear plastic bag. Due to the illegal nature of the gun and ammunition as it relates to ownership by WILLIAM JONES, a convicted felon, and pursuant to Title 18, United States Code 922(g)(1), Agents removed the gun and ammunition from the residence.

36. While in the basement, referred to in paragraph 35, your affiant noticed that multiple computers were located on a shelf above the ammunition. Your affiant obtained a photograph of this shelf.

37. Following removal of the gun and ammunition, referred to in paragraph 35, WILLIAM JONES arrived at the residence as Agents returned upstairs. Your affiant

encountered WILLIAM JONES at the entrance and asked to speak with him. WILLIAM JONES suggested speaking in a nearby vehicle and your affiant agreed. Your affiant, SA Abramovitz, and WILLIAM JONES then proceeded to your affiant's unmarked HSI vehicle. Your affiant and WILLIAM JONES sat in the back seat while SA Abramovitz sat in the driver's seat. Your affiant verbally advised WILLIAM JONES of his Miranda rights and that he was not under arrest and he affirmed his understanding. Your affiant then informed WILLIAM JONES that Agents were present to discuss an issue related to the internet, financial transactions, and child exploitation. Your affiant asked WILLIAM JONES what he understood child pornography to be and he stated it was children in sexual acts. WILLIAM JONES agreed that a minor was defined as anyone under the age of 18 years. Your affiant then informed WILLIAM JONES that it was believed he had purchased and downloaded password-protected files containing child pornography when he lived in Meadville, PA. WILLIAM JONES denied this activity and then stated that he didn't recall purchasing and downloading files containing child pornography but if your affiant said he had done so then he must have.

38. At the conclusion of the interview referred to paragraph 37, your affiant asked WILLIAM JONES for written consent to search his computers to make sure that no child pornography was present. Without hesitation, WILLIAM JONES agreed to provide written consent for his current Samsung mobile telephone and his current IBM Thinkpad Laptop computer. Your affiant also asked WILLIAM JONES for consent to search the computers observed in his basement and he stated that he had destroyed and thrown away the hard drives to these computers by busting them up. Agents and WILLIAM JONES exited the vehicle and returned to the residence and your affiant asked WILLIAM JONES if he would show your affiant the computers in the basement to confirm there were no hard drives contained in them.

WILLIAM JONES agreed and led your affiant and SA Abramovitz downstairs to the location of the computers referred to in paragraph 36. Your affiant then observed there were two (2) tower computers, one (1) laptop computer, and one (1) tablet computer on the shelf. WILLIAM JONES removed the case of two (2) tower computers and your affiant observed a hard drive contained inside one (1) with no apparent damage. WILLIAM JONES stated that he intended to discard these computers. Your affiant again asked for consent to search these computers for the presence of child pornography and WILLIAM JONES paused. Your affiant asked WILLIAM JONES what he was thinking and he didn't immediately answer. WILLIAM JONES then informed Agents that he was hesitant to cooperate with law enforcement because he had done so in the past and it resulted in a maximum sentence. WILLIAM JONES also informed Agents that he did not want to do anything to disrupt his life. Your affiant asked what was on the computers and WILLIAM JONES did not answer. Your affiant reminded WILLIAM JONES that written consent to search his computers was being requested to make sure that no child pornography was present. WILLIAM JONES then indicated he wanted to retain the computers and Agents informed him that they needed to detain the computers. WILLIAM JONES then proceeded to remove the hard drive from one (1) tower computer and hand it to Agents. WILLIAM JONES then retrieved the laptop computer and tablet computer from the shelf and handed it to Agents.

39. While in the basement with WILLIAM JONES, referred to in paragraph 38, HSI Special Agents Robert Connelly and Brandon Wargo came downstairs and were present when WILLIAM JONES repeated to Agents that he had previously destroyed hard drives.

40. A few minutes following the events described in paragraphs 38 and 39, Agents and your affiant were present in the living room of the residence with WILLIAM JONES and

Ching Hsieh. At this time, WILLIAM JONES repeated that he intended to throw away the computers in the basement and indicated that his wife had knowledge of this intention.

41. Based upon the multiple statements of WILLIAM JONES regarding his previous destruction of hard drives, and intention to destroy his computers, WILLIAM JONES' statement that he must have downloaded files containing child pornography, and WILLIAM JONES' confirmation that he had owned the hard drive and computers in his basement while living in Meadville, PA, Agents detained one (1) hard drive from a tower computer, one (1) laptop computer, and one (1) tablet computer to prevent the destruction of potential evidence.

42. Your affiant asked WILLIAM JONES if the computers, referred to in paragraphs 36 and 38, were from the time he had lived in Meadville, PA and he confirmed that they were. WILLIAM JONES added that he had them for years.

43. During the consent search of the Samsung cell phone belonging to WILLIAM JONES, referred to in paragraph 38, your affiant observed that the telephone number of this device is 814-720-7866 which matches the telephone number contained in the payment processing information, referred to in paragraph 22.

44. On September 23, 2019, your affiant applied for and was issued a federal search warrant for the electronic devices referred to in paragraph 41. This search warrant was executed on September 25, 2019. A subsequent review of the contents of the Seagate Hard Drive revealed multiple e-mail addresses associated with Google, Inc. including "contactwilliamjones@gmail.com" and "wj1234wj@gmail.com", which contains the same letters and is similar to the e-mail address contained in the original lead; "1234wjwj@gmail.com", referred to in paragraph 22. In addition, this hard drive was found to

contain internet history records with the term “gmail” and corresponding access dates between approximately February 5, 2014 and January 16, 2018.

45. A review of the contents of the laptop computer, referred to in paragraph 38 as an IBM Thinkpad Laptop, and now fully identified as a Lenovo Thinkpad Laptop, revealed multiple e-mail addresses associated with Google, Inc. including “contactwilliamjones@gmail.com” and “wj1234wj@gmail.com”, which contains the same letters and is similar to the e-mail address contained in the original lead; “1234wjwj@gmail.com”, referred to in paragraph 22. In addition, this laptop computer was found to contain internet history records with the term “gmail” and corresponding access dates between approximately September 6, 2016 and July 19, 2019.

46. Based on my investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, your affiant knows that during the course of investigations associated with “Website M” in the Western District of Pennsylvania, at least one (1) other individual has confirmed the process of obtaining child pornography that is described in paragraph 12 which involves downloading an encrypted archive file then receiving the password to this archive file to their e-mail address after purchase. Your affiant also knows that this individual has indicated that child pornography may not be saved because once the password is purchased and received, the individual can always download the encrypted archive again.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO, RECEIVE, POSSESS,
AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY**

47. Based on my investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who receive, possess,

and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography

images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.⁴

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including e-mail addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography

⁴ See United States v. Carroll, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also United States v. Seiver, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., United States v. Allen, 625 F.3d 830, 843 (5th Cir. 2010); United States v. Richardson, 607 F.3d 357, 370–71 (4th Cir. 2010); United States v. Lewis, 605 F.3d 395, 402 (6th Cir. 2010).)

for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

48. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “Wi-Fi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer using telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily,

inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices, which plug into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Individuals can easily store, carry or conceal media storage devices on their persons. Individuals also often carry Smartphones and/or mobile phones.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where an individual uses

online storage, however, law enforcement can find evidence of child pornography on the user's computer, smartphone or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information such as the traces of the path of an electronic communication may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information exists indefinitely until overwritten by other data.

STORED WIRE AND ELECTRONIC COMMUNICATION ACCESS

49. Title 18, United States Code, Chapter 121, Sections 2701 through 2712, is entitled the "Stored Communications Act" (SCA). Section 2703 of the SCA sets forth the procedure that federal and state law enforcement officers follow to compel disclosure of various categories of stored electronic information from service providers. This Court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by Section 2711(3)(A)(i) of the SCA. This application is made pursuant to the Stored Communications Act and the Federal Rules of Criminal Procedure.

50. Based on the foregoing, and consistent with Rule 41(e)(2)(B), your affiant is applying for a Search Warrant that would permit seizing, imaging, or otherwise copying of all e-

mails, messages, and other information and electronic data that may be stored and found on Google, Inc. servers which pertain to Google, Inc. e-mail account **1234wjwt@gmail.com** that reasonably appears to contain some or all of the evidence described in the Search Warrant and would authorize a later review of the information consistent with the Search Warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire information, that might expose many parts of the information to human inspection in order to determine whether it is evidence described by the Search Warrant.


REQUEST FOR SEALING OF WEBSITE/AFFIDAVIT

51. It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be provided to WILLIAM JONES). Sealing is necessary because the items and information agents intend to seize are relevant to an ongoing investigation and agents will not search all of the targets of this investigation at this time. Based upon my training and experience, your affiant has learned that online criminals actively search for criminal affidavits and Search Warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through forums. Premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on this continuing investigation and may jeopardize its effectiveness by alerting potential targets to the existence and nature of the investigation, thereby giving them an opportunity to flee, or to destroy or tamper with evidence.

CONCLUSION

52. Based on the foregoing, there is probable cause to believe that the federal criminal

statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment A, are located at the locations also described in Attachment A. I respectfully request that this Court issue a Search Warrant for the locations described in Attachment A, authorizing the seizure and search of the items also described in Attachment A.



Jason Adams
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 16th day of October 2019.



UNITED STATES MAGISTRATE JUDGE